ThreatQuotient

ThreatQuotient for HCP Connector Guide

Version 1.1.2

Friday, May 8, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: Support.threatq.com

Phone: 703.574.9893

Warning and Disclaimer

ThreatQuotient, Inc. provides this document "as is", without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Contents

Versioning

- Integration Version: 1.1.2
- ThreatQ Version: 4.20.0 or greater

Operating System	OS Version	Python Version	Notes
RedHat/CentOS	7	2.7.12	N/A
Ubuntu	16.04	2.7.12	This has not been tested.
Windows	2012R2/10	2.7.12	This has not been tested.

Introduction

The Hortonworks Cybersecurity Platform (HCP) is an open source threat intelligence platform that collects telemetry events from network sensors (e.g. proxies), matches indicators from those events to threat intelligence feeds, and alerts SOC analysts of potential intrusions. It can be used as a SIEM, as well as a TIP. HCP is a framework that encompasses many different applications and services and usually sits on top a cluster with these applications: HDFS, YARN, MapReduce, Hive, HBase, Zookeeper, Spark, Zeppelin Notebooks, Solr or Elasticsearch, Storm, Kafka, NiFi, and Metron.

This custom connector integrates ThreatQ with the Kafka brokers installed in HCP. Kafka is a messaging service which is used for handling high volume real-time data feeds, and is one of the entry points for data into HCP.

The connector runs a saved search in ThreatQ, parses the indicators from the search, and sends them as individual messages to a Kafka endpoint in the Metron API that is installed as part of HCP.

Installation

This package is available in `.tar.gz` and `.whl` formats, and can be installed from the ThreatQ integrations repository.

To install the `.tar.gz` or `.whl` formats:

```
pip install /path/to/file.extension
```

Executing the Driver

This package comes with a driver called `tq-conn-hcp-kafka`. After installing with `pip` or `setup.py`, a script stub will appear in `/usr/bin/tq-conn-hcp-kafka`.

To execute the feed just use:

```
tq-conn-hcp-kafka -c /path/to/config/directory/ -ll

/path/to/log/directory/ -v VERBOSITY_LEVEL
```

The driver will run once, where it will connect to the TQ instance and will install the UI component of the connector. After installation, the user will need to go into the connector UI and configure the required fields.

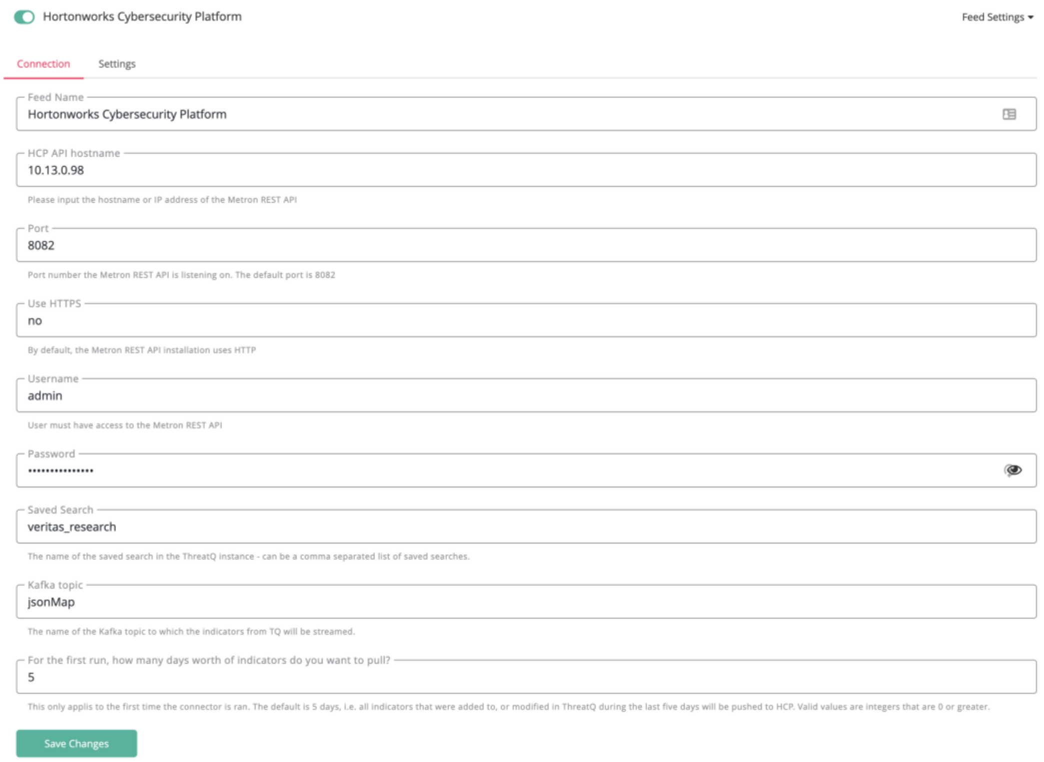
Configuration

> ***Note:*** *ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other feed-related credentials.*

To configure the connector:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the connector under the **Labs** tab.
3. Click on the **Feed Settings** link for the connector.
4. Under the Connection tab, enter the following configuration parameters:

Parameter	Description
HCP API Hostname	Hostname or IP address of the Metron REST API.
Port	Port number the Metron REST API is listening on. The default port is 8082.
Use HTTPS	By default, the Metron REST API installation uses HTTP.
Username	The provided username for the Metron API.
Password	The password for logging to the Metron API.
Saved Search	The name of the saved search in the ThreatQ instance - can be a comma separated list of saved searches.
Kafka Topic	The name of the Kafka topic to which the indicators from ThreatQ will be streamed.
For first run, how many days worth of indicators do you want to pull?	The default is 5 days, i.e. all indicators that were added to, or modified in ThreatQ during the last five days will be pushed to HCP. Valid values are integers that are 0 or greater. This only applies to the first time the connector is ran.



Feed Name: Hortonworks Cybersecurity Platform

HCP API hostname: 10.13.0.98

Please input the hostname or IP address of the Metron REST API

Port: 8082

Port number the Metron REST API is listening on. The default port is 8082

Use HTTPS: no

By default, the Metron REST API installation uses HTTP

Username: admin

User must have access to the Metron REST API

Password: •••••••••••••••

Saved Search: veritas_research

The name of the saved search in the ThreatQ instance - can be a comma separated list of saved searches.

Kafka topic: jsonMap

The name of the Kafka topic to which the indicators from TQ will be streamed.

For the first run, how many days worth of indicators do you want to pull?: 5

This only applis to the first time the connector is ran. The default is 5 days, i.e. all indicators that were added to, or modified in ThreatQ during the last five days will be pushed to HCP. Valid values are integers that are 0 or greater.

5. Click on Save Changes.
6. Click on the toggle switch to the left of the connector name to enable the connector.

CRON

Automatic CRON configuration has been removed from this script. To run this script on a recurring basis use CRON or some other jobs scheduler. The argument in the CRON script must specify the config and log locations.

Add an entry to your Linux crontab to execute the connector at a recurring interval. Depending on how quickly you need updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

In the example below, the command will execute the connector at the top of every hour.

- Log into your ThreatQ host via a CLI terminal session.
- Enter the following command:

```
crontab -e
```

This will enable the editing of the crontab, using vi.

Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

- To push added, or updated indicators from ThreatQ to Kafka, you can configure a CRON entry to run the connector. Depending on how quickly you want updates, this can be run multiple times a day (no more than once an hour) or a few times a week.

  Hourly Example

```
 0 * * * * /usr/bin/tq-conn-hcp-kafka -c
/path/to/config/directory/ -ll /path/to/log/directory/ -v
VERBOSITY_LEVEL
```

- Save and exit cron.

Command Line Arguments

This connector supports the following custom command line arguments:

Argument	Description
`-h, --help`	Shows this help message and exits.

`-ll LOGLOCATION, --`
`loglocation LOGLOCATION`
	Sets the logging location for the connector. The location should exist and be writable by the current. A special value of 'stdout' means to log to the console (this happens by default).

`-c CONFIG, --config CONFIG`	This is the location of the configuration file for the connector. This location must be readable and writable by the current user. If no config file path is given, the current directory will be used. This file is also where some information from each run of the connector may be put (last run time, private oauth, etc.)

`-v {1,2,3}, --verbosity`
`{1,2,3}`
	This is the logging verbosity level. The default is 1 (Warning).

`-ep, -external-proxy`	This allows you to use the proxy that is specified in the ThreatQ UI.
`-ds, --disable-ssl`	Adding this flag will disable SSL verification when contacting the Metron API.
`-hist, --historical`	Push to HCP all indicators created or updated in the past X days, where X is

Argument	Description
	the number of days provided in the ThreatQ config UI.

Change Log

Version	Details
1.1.2	• Updated the TL search library with the latest version which is v1.0.10 • Modified parsing of the data returned from the TL search • Changed the ThreatQ IP that is sent to Metron to the actual IP/hostname of ThreatQ
1.1.0	Initial Release